CLAIMS

What is claimed is:

1. A merchant who accepts credit cards, debit cards, or smart cards consisting of multi-purpose, oil company or department store cards, franchisee cards, or travel and entertainment cards, or retail store cards, or any magnetic striped or smart card comprised of:
Card present, where the cardholder is present at the point of sale either via a magstripe card swipe terminal, key input pad, card insertion machine, or voice authorization or other access device pursuant to 18 USC section 1029.

Card not-present, where the cardholder is not physically present at the point of sale at the merchant's location and either employs a mail order/telephone order (MOTO) transactional process for goods or services via a magstripe terminal, card insertion machine or , voice authorization, computer terminal, telephone, telephony, facsimile, postal mail, courier or other access device pursuant to 18 USC 1029 on the merchant's end.

Telephone companies, Utility companies, or pay for television companies who extend services based upon a cardholders verifiable credit history to include but not be limited to Geographical or regional jurisdictions.

Commercial Banks and other Financial Institutions who extend services based upon a cardholders verifiable credit histories to include but are not limited too savings and loans, mortgage banks, credit unions, auto loans, commercial loans, Credit Bureaus, Boat loans, Cash advance locations, etc.

Government Documents and Benefits who extend benefits and services based upon a card holders verifiable credit history to include but not be limited to Social security administration, Veteran's Administration, Department of motor vehicle, Internal Revenue Service, Federal Aviations Administration, Homeland security, Voter registration, Airports.

Medical and Insurance and Securities industry enterprises who extend services based upon a card holders verifiable credit history to include

but not be limited to Birth Certificates, Death Certificates, Medicare/Medicaid, Plastic Surgeons Associations, Stocks and Bonds, Life/Death/Annuity and Universal policy distributors.

2. That the link between a merchant's magstripe swipe terminal, card insertion machine, PIN pad, or other access device on the one hand and an external or internal modem of a merchant's in-store computer server on the other hand by physical medium or wireless transmission.

3. The merchant's system according to claim 1 provides at least one in store video display terminal or other output device, e.g. printer, notebook, projector, video telephone, or camera phone that supports monochrome display adapters (MDA), Hercules Graphics cards (HGC), Color graphics adapter (CGA), Enhanced Graphic Adapters (EGA), Video Graphics Array (VGA), or super and ultimate VGA (SVGA), light emitting diode (LED), Liquid crystal display (LCD), High definition television (HDTV), or plasma display capabilities.

4. The merchant's system according to claim 1 provides at least one in-store computer server equipped with either an external or internal modem or high speed connection and is supported by an interoperable operating system and links to the remote SAN server across a WAN.
5. That the pre-authenticated method and process is linked to various independent objective public, private, or internal data-bases whereupon a query is performed on sensitive data to locate a match. Examples of databases include, but are not limited to, Bank identification numbers (BIN), social security administration, department of justice, mortuary records, worldwide telephone directory, State motor vehicle records, public records, national courts and court records, nationwide criminal records checks, state criminal records checks, state and federal inmate locater, Docusearch, Vital records information, Plastic Surgeons Associations, Military search, cemeteries and obituaries, Freedom of information, Federal bureau of investigation, Drug Enforcement Administration, Secret Service, Securities and Exchange Commission, Health and Human Services, On-line hospital and health systems, Office of the Pardon Attorney, Foreign Embassies, People Locator, and any and all other records searches available to produce an authenticated customer.

7. That the SAN database is a uniquely scripted Structured Query Language (SQL) either commercial or proprietary that maps a primary key of either (1) a non-checking account number or it's pointer, or (2) a facial image, or it's pointer, of each primary and/or secondary acccount holder with a foreign key of any reverse combination of any of the foregoing.

8. That the account holder's personal and sensitive data is captured by secure web site, instant messaging, facsimile, postal mail, courier, or telephony equipment or any other web based capturing interface and is returned from a previously authenticated process and remote database to the merchant's video display output device at some point in the future after data capture.

9. That the account holder's facial image is captured by web camera, digital camera, camera phone, internet protocol camera, video camera, watch camera, or any other digital photographic device other than a CMOS scanner.

10. That the pre-authenticated method and process implements a facial recognition software for capturing and matching account holder's visages to be displayed at some point in the future to the merchant's output display device after image capture.

11. That the method and process employs a concurrent or approximate concurrent link in the form of a request to both an account approving authority or clearinghouse as well as to a remote database and returns both an authorization number supplied by said account approving authority or clearinghouse as well as a pre-authenticated static or dynamic digital photographic image supplied by said database whereas both the textual data and video image will be displayed simultaneously at the merchant's POS.

12. That the individual unique facial image of each individual primary and/or secondary account holder is returned from a previously authenticated process and database to the merchant's video display output device.

13. That the merchant's POS has an audio output device that produces a pre-determined audio signal that is unique and ubiquitous for each authenticated customer approximately following each card transaction associated with this embodiment.